CHAPTER 1

Introduction

There are two primary choices in life: to accept conditions as they exist, or accept the responsibility for changing them.

—Denis Waitley

Given that security breaches and intrusions continue to be reported daily across organizations of every size, is information security really effective? Given the rapid evolution of new technologies and uses, does the information security group even need to exist?

Obviously, this is a somewhat rhetorical question. I cannot imagine that any sizeable organization would operate well without an information security function. The real issue is whether the information security group should continue to exist as it does today, with its traditional mission and vision.

As information security professionals, we should be asking ourselves pointed questions if we wish to remain valuable and relevant to our organizations. Why do we exist? What should our role be? How are new consumer technologies shaping what we do—and can we shape the world of the consumer? How is the evolving threat landscape shaping us—and can we shape the threat landscape? Given the bewildering pace at which technology changes and new threats appear, how do we focus and prioritize our workload? What skills do we need?

Traditionally, information security groups within businesses and other organizations have taken a relatively narrow view of security risks, which resulted in a correspondingly narrow charter. We focused on specific types of threats, such as malware. To combat these threats, we applied technical security controls. To prevent attacks from reaching business applications and employees' PCs, we fortified the network perimeter using firewalls and intrusion detection software. To prevent unauthorized entry to data centers, we installed physical access control systems. Overall, our thinking revolved around how to lock down information assets to minimize security risks.

Today, however, I believe that this narrow scope not only fails to reflect the full range of technology-related risk to the business, it may be detrimental to the business overall. Because this limited view misses many of the risks that affect the organization, it leaves areas of risk unmitigated and therefore leaves the organization vulnerable in those areas. It also makes us vulnerable to missing the interplay between risks and controls: By implementing controls to mitigate one risk, we may actually create a different risk.

As I'll explain in this book, we need to shift our primary focus to adopt a broader view of risk that reflects the pervasiveness of technology today. Organizations still need traditional security controls, but they are only part of the picture.

There are several reasons for this. All stem from the reality that technology plays an essential role in most business activities and in people's daily lives.

Technology has become the central nervous system of a business, supporting the flow of information that drives each business process from product development to sales. The role of technology in peoples' personal lives has expanded dramatically, too, and the boundaries between business and personal use of technology are blurring. Marketers want to use social media to reach more consumers. Employees want to use their personal smartphones to access corporate e-mail.

Meanwhile, the regulatory environment is expanding rapidly, affecting the way that information systems must manage personal, financial, and other information in order to comply—and introducing a whole new area of IT-related business risks.

Threats are also evolving quickly, as attackers develop more sophisticated techniques—often targeted at individuals—that can penetrate or bypass controls such as network firewalls.

In combination, these factors create a set of interdependent risks related to IT, as shown in Figure 1-1.

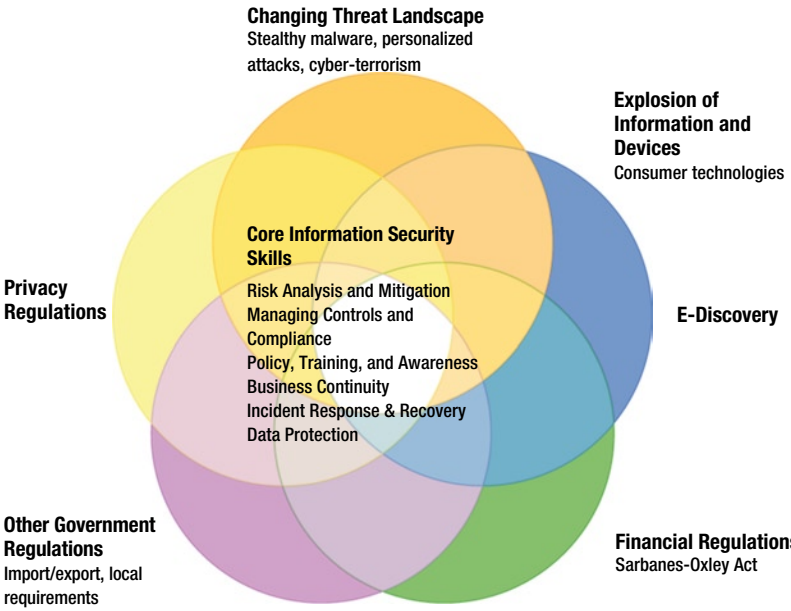

Figure 1-1. *Interdependent risks related to IT. Source: Intel Corporation, 2012*

Traditional security thinkers would respond to this by saying "no" to any technology that introduces new risks. Or perhaps they would allow a new technology but try to heavily restrict it to a narrow segment of the employee population. Marketers should not engage consumers with social media on the company's web site, because this means accumulating personal information that increases the risk of noncompliance with privacy regulations. Employees cannot use personal devices because they are less secure than managed business PCs.

The reality is that because IT is now integrated into everything that an organization does, security groups cannot simply focus on locking down information assets to minimize risk. Restricting the use of information can constrain or even disable the organization, hindering its ability to act and slowing its response to changing market conditions. A narrow focus on minimizing risk therefore introduces a larger danger: it can threaten a business's ability to compete in an increasingly fast-moving environment.

Protect to Enable

To understand how the role of information security needs to change, we need to reexamine our purpose. We need to *Start with Why*, as author Simon Sinek argues convincingly in his book of the same name (Portfolio, 2009). Why does the information security group exist?

As I considered this question and discussed it with other members of Intel's internal information security team, I realized that we needed to redefine our mission. Like the IT organization as a whole, we exist to enable the business—to help deliver IT capabilities that provide competitive differentiation. Rather than focusing primarily on locking down assets, the mission of the information security group must shift to enabling the business while applying a reasonable level of protection. To put it another way, we provide the protection that enables information to flow through the organization.

The core competencies of information security groups—such as risk analysis, business continuity, incident response, and security controls—remain equally relevant as the scope of information-related risk expands to new areas like privacy and financial regulations. But rather than saying "no" to new initiatives, we need to figure out how to say "yes" and think creatively about how to manage the risk.

Within Intel, the role of our security group has evolved toward this goal over the past several years, as we have helped define solutions to a variety of technology challenges.

Starting in 2002, we recognized that implementing wireless networks within Intel's offices could help make our workforce more productive and increase their job satisfaction by letting them more easily connect using their laptops from meeting rooms, cafeterias, and other locations. At the time, many businesses avoided installing wireless networks within their facilities because of the risk of eavesdropping or because of the cost. We learned pretty quickly that when we restricted wireless LAN deployments or charged departments additional fees to connect, we actually generated more risks. This was because the departments would buy their own access points and operate them in an insecure fashion. We recognized that the benefits of installing wireless LANs across the company outweighed the risks, and we mitigated those risks using security controls such as device authentication and transport encryption. Today, our employees see wireless LANs as indispensable business tools.

A more recent example: for years, Intel—like many other organizations—didn't allow employees to use personal smartphones for business, due to privacy concerns and risks such as the potential for data theft. However, we experienced growing demand from employees who owned personal smartphones, and we realized that letting them use these consumer devices to access e-mail and other corporate systems would help boost employee satisfaction and productivity.

By working closely with Intel's legal and human resources (HR) groups, we defined security controls and usage policies that enabled us to begin allowing access to corporate e-mail and calendars from employee-owned smartphones in early 2010. The initiative has been highly successful, with a massive uptake by employees, overwhelmingly positive feedback, and proven productivity benefits (Evered and Rub 2010, Miller and Varga 2011).

The transformation within Intel's information security group is reflected in changes to our mission statement and top priorities over the years, as shown in Figure 1-2. In 2003, our internal mission statement reflected the traditional focus and scope of information security organizations: our overarching goal was to protect Intel's information assets and minimize business disruption.

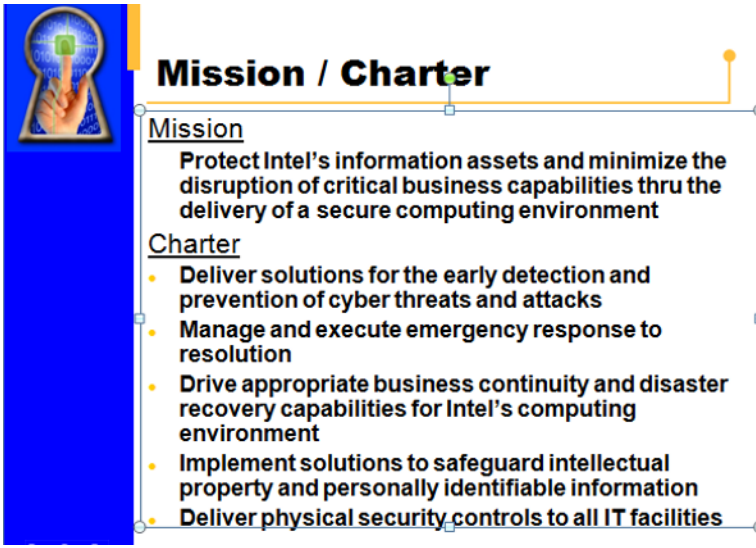

Figure 1-2a. *How the mission of Intel's Information Security Group has changed: the mission and priorities in 2003. Source: Intel Corporation, 2012*

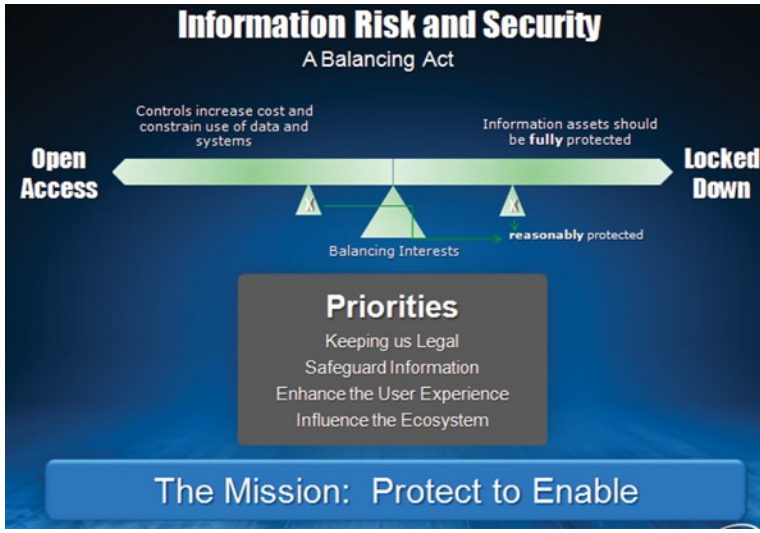

Figure 1-2b. *How the mission of Intel's Information Security Group has changed: the mission and priorities in 2012. Source: Intel Corporation, 2012*

By late 2011, we had changed our mission to Protect to Enable. Our primary goal is now to find ways to enable the business while providing the protection that's necessary to reduce the risk to an acceptable level.

I think of information security as a balancing act. We try to find the right balance between providing open access to technology and information—to enable the business—and locking down assets. Providing open access allows greater business agility. The business can move more quickly with fewer restrictions. Employees can work more freely, and the faster flow of information allows the company to grow and transform.

Within this mission, our priorities reflect the shift in emphasis and our broader view of information risk, as well as the way that the security landscape has changed since 2003.

- *Keeping the company legal*. Compliance, which didn't merit a mention in our 2003 priority list, surged to the top of the list in 2011. This is driven by the growing regulatory environment and the resulting impact on IT.
- *Safeguarding information*. Protecting information assets—our overall mission in 2003—has not disappeared from our list of priorities. However, it has become only one of several items on the list.
- *Enhancing the user experience*. Positioning this as a priority might seem counterintuitive. After all, traditional security groups are better known for blocking users' access. But it's essential to keep the user's experience in mind when devising security policies and controls. If we make it difficult or time-consuming for users to follow security policies, they'll ignore them. In a competitive industry, a delay of

10 minutes can mean losing a sale. When faced with a choice of following policy or losing a customer's business, which do you think a salesperson would choose?

- *Influencing the ecosystem*. In most industries, companies are collaborating more—they are partnering, specializing, and outsourcing. The growing need to exchange information means that compromise to one company can more easily spread to business partners. However, there are also opportunities for businesses to collaborate on security initiatives and standards that help the industry overall; think of the benefits to healthcare companies of being able to securely exchange patient information. Each company benefits by influencing the ecosystem to become more secure.

Though this list represents our current priorities at Intel, I hope that it may be useful for information security groups at other organizations to think about how these priorities relate to their own businesses.

The balancing point between providing open access and locking down assets depends on the organization's appetite for risk. At Intel, informed risk-taking is part of a culture that is designed to help foster innovation. Other businesses may have a different level of risk tolerance.

To analyze the context that has led to our security mission and top priorities, I'll explore some of the key changes in the landscape that affect how we view and manage risk: the rapidly expanding regulatory environment, the emergence of new devices and technologies, and the changing threat landscape.

Keeping the Company Legal: The Regulatory Flood

Until the early 2000s, I didn't see regulatory compliance as a top priority for information security. That's simply because there weren't many regulations that impacted IT, at least in the United States. There were a few exceptions that affected a subset of companies, including Intel, such as controls on certain high-tech exports. And in European countries, there were already regulations that sought to protect personal information. But in general, IT groups didn't have to dedicate much of their time—or budget—to regulatory compliance.

The change in the last decade has been extraordinary. We have seen a flood of new regulations implemented at local, national, and international levels. They affect the storage and protection of information across the entire business, from the use of personal information for HR and marketing purposes, to financial data, to the discovery of almost any type of document or electronic communication in response to lawsuits. And with growing concerns about cyberwarfare, cyberterrorism, and hacktivism, several countries are evaluating additional cybersecurity legislation in an attempt to protect critical infrastructure and make industries more accountable for strengthening security controls.

In most cases, these regulations do not aim to specifically define IT capabilities; however, because information is stored electronically, there are huge implications for IT. The controls defined in the regulations ultimately must be implemented in the organization's systems. These systems include more than just technology: they consist of

people, procedures, devices, and applications. The business risk includes a significant IT-related component, but we must take a holistic view of risk management. Noncompliance can damage a company's brand image, profitability, and stock price—not just through resulting legal problems, but through bad publicity.

Let's take a brief look at some of the key areas and regulations that are having the biggest impact.

Privacy: Protecting Personal Information

For many US companies, the wake-up call was the California data security breach notification law (State Bill 1386), which became effective in 2003. A key aspect of this law requires companies that store personal information to notify the owner of the information in the event of a known or suspected security breach. Businesses could reduce their exposure, as well as the risk to individuals, by encrypting personal data.

After this, other states quickly followed suit, implementing regulations that generally follow the basic tenets of California's original law: companies must promptly disclose a data breach to customers, usually in writing.

In addition, federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), have addressed specific categories of personal information. Further regulations have been added in other countries, too, such as the updated data-protection privacy laws implemented in Europe (European Commission 2011, 2012).

The implications of these local and national regulations extend beyond geographical boundaries. As companies do more business online, they're increasingly likely to acquire and store information about customers from other countries—and find they also need to comply with regulations around the world. For example, citizens of European countries may register on the web site of a US business so that they can receive information and product updates.

The issue becomes even more complex when businesses outsource application development or HR functions to providers located in yet another country. Now, software developers in India may be building and operating the systems that collect information about Europeans for US companies, making it even more difficult for businesses to navigate compliance with all relevant privacy regulations.

Personalization versus Privacy

Privacy concerns are set to become even more important over time, as businesses increasingly seek to create online experiences tailored to the needs of individual users. The more a business knows about each individual, the more it can personalize services and offer targeted advertising based on income and preferences.

Many users also like personalized services. If a web site "remembers" them, they don't need to enter the same information each time they visit the site, and they're more likely to see content and offers relevant to their needs. In fact, companies may be at a disadvantage if they don't personalize services, because users may prefer a web site from a competitor that offers a more streamlined experience.

However, there's an inevitable conflict between personalization and privacy. The personalization trend is fueling the growth of an industry focused on collecting, analyzing, and reselling information about individuals. This industry existed long before the Web; personal information has been used in mass-mailing campaigns for decades. However, the Web is both increasing demand for this information while providing new ways to collect it. Companies now have opportunities to collect information from multiple online sources, correlate and analyze this information, and then sell it to others. And of course, consumers' fears that information will be lost or misused have increased accordingly.

For businesses, however, offering personalized services also can increase compliance concerns. As companies store more personal information, they are responsible for safeguarding that information and are liable for any loss or compromise. In many parts of the world, companies are also required to explain why they are collecting personal data, how they are protecting it, and how long they will keep it.

We can expect continuing tension due to conflicting desires for personalization and privacy—and more regulation as a result. Governments clearly believe that businesses cannot be relied upon to regulate themselves, so they will continue to add regulations designed to protect the privacy of individuals. Meanwhile, businesses will seek new ways to collect more information so that they can further personalize services. Developing compliance strategies and guidelines becomes even more pressing.

Financial Regulations

Financial regulation surfaced as a top priority in the United States with the Sarbanes-Oxley Act (SOX), which emerged from the public outrage over corporate and financial accounting scandals at companies such as Enron and WorldCom. These scandals cost investors billions of dollars and damaged public confidence. To help avoid similar catastrophes in future, SOX imposed financial tracking requirements designed to ensure that a company's financial reporting is accurate and that there hasn't been fraud or manipulation. Once enacted, SOX required publicly held companies to meet specific financial reporting requirements by the end of 2004.

Though the Sarbanes-Oxley Act doesn't mandate specific technology controls, it has major implications for IT. Ensuring financial integrity requires controls to be implemented within everyday financial processes. In practice, this means they must be enforced within the IT applications and infrastructure that support those processes. Purchases above specific thresholds may require approval from the finance group; the underlying applications have to support this workflow, and to be sure the applications function correctly, businesses need to establish the integrity of the underlying computer infrastructure. Compliance with financial regulations therefore creates a series of IT requirements, from making sure that applications provide the right functionality to implementing access controls and updating software. This compliance comes at a steep cost: enterprises surveyed by Gartner, Inc. (2005) estimated that 10 to 15 percent of their entire IT budgets in 2006 would be spent on financial regulatory compliance.

e-Discovery

Regulations governing the discovery of information for litigation purposes officially extended their reach into the electronic realm in 2006. That's when the US Supreme Court's amendments to the Federal Rules of Civil Procedure explicitly created the requirement for e-discovery—the requirement to archive and retrieve electronic records such as e-mail and instant messages.

This created an immediate need not just to archive information, but to automate its retrieval. This is because records must be produced in a timely way—and manual retrieval would take too long and be prohibitively expensive. The business risks of noncompliance are considerable: unlike many countries, US practice allows for potentially massive information disclosure obligations in litigation. Companies that fail to meet e-discovery requirements may experience repercussions that include legal sanctions. The implications are correspondingly onerous. Lawsuits may draw on information that is several years old, so businesses must have the capability to quickly search and access archived information as well as current data. E-discovery is further complicated by the growth of cloud computing models such as software as a service (SaaS). As organizations outsource more business processes and data to cloud service suppliers, they need to ensure that their suppliers comply with their e-discovery needs.

Expanding Scope of Regulation

The regulatory universe continues to expand, with the likelihood of more regulations that explicitly address IT, as new technologies emerge and governments try to control its use and inevitable misuse.

Some technology-specific regulations have been triggered by specific events. In India, for example, after terrorists used unsecured Wi-Fi access points to communicate information about their attacks, the government created a legal requirement that any access point must be secured (Government of India Department of Telecommunications 2009).

In other countries, businesses that operate unsecured Wi-Fi access points—a common way to provide Internet access for visitors—may find themselves facing other legal problems. For example, unscrupulous individuals may tap into the network to access web sites for purposes such as illegally downloading music or pornography. Access appears to originate from the company hosting the access point, which may then find itself on the receiving end of correspondence or raids from the music industry or government agencies.

The Rapid Proliferation of Information and Devices

The computing environment is growing as rapidly as the regulatory environment. The sheer volume of information is exploding, and it is being stored across a rapidly growing array of portable computing devices.

This is a dramatic acceleration and expansion of a long-running trend that began when businesses first started equipping employees with desktop and then laptop PCs. Now, employees are using millions of smartphones and other devices, such as tablets, to access and store information.

At the same time, the boundaries between work and personal technology are dissolving. Whether businesses officially allow it or not, employees are increasingly using their personal devices for work—sending e-mails from and storing information on their personal smartphones and computers. Furthermore, people may forward e-mail from business accounts to personal accounts created on external systems—without considering that when they signed up for the personal account, they agreed to a license that allows the external provider to scrutinize their e-mails.

The use of personal technology can considerably enhance business productivity because employees can now communicate from anywhere at any time. However, this also creates a more complex, fragmented environment with more potential points of attack. Information is now exposed on millions of new devices and disparate external networks, many of which do not have the same type of security controls as corporate PCs—and all of which are outside corporate network firewalls.

Statistics show that malware producers are already responding to the growing popularity of these new devices; security firm McAfee (owned by Intel) (2011) reported significant growth in malware targeting mobile devices during the second quarter of 2011—with a 76 percent increase in malware aimed at devices running Google's Android software.

We can expect an ever-growing variety of networked devices. In fact, in the not too distant future, almost any device with a power supply might have a network address and be capable of communicating—and being attacked—over the Internet.

Already, cars contain dozens of control computers that communicate over internal networks. Some have IP addresses, and with a mobile phone app, owners can remotely control a variety of functions, including starting the car. Researchers have shown that it's possible to insert malicious code into a car's computers to control the brakes and accelerator. They have also shown that navigation systems in cars can be spoofed to send the driver to the wrong destination. Consider the possibilities if a family member is driving the car, or a company executive.

The boundaries between work and personal lives are dissolving in other ways, too. Employees store more information on the Internet—on business and consumer social media sites, for example—than ever before. These sites have become powerful tools for communicating with audiences outside the corporate firewall.

However, just as there's an industry gathering and analyzing personal information for marketing purposes, information on the Web can be used for competitive intelligence or for less legitimate purposes. Users store snippets of information in multiple places on the Web. Though each of these snippets may not provide much information, when pieced together, they can provide new intelligence—not just about the individual, but also about the organization to which the person belongs. Each item is like a single pixel in a digital picture. Alone, it doesn't convey much information; but step back—aggregating information from a wider range of sources—and multiple pixels combine to form a portrait. In the same way, pieces of information strewn across a variety of unrelated web sites—the name of a department, workmates, pet names that might be used as passwords—can be linked together to create a picture of an individual and used for malicious purposes.

The Changing Threat Landscape

The threat landscape is evolving rapidly, with an increase in highly organized and well-funded groups capable of executing sustained attacks to achieve long-term goals. Such a group is thought to have created Stuxnet, a sophisticated worm that targeted specific industrial systems and is suspected to have set back the Iranian nuclear program by as much as two years. These attackers, generally known as *advanced persistent threats* (APTs), were originally focused mainly on governments. However, more recent data indicates that APTs are now targeting private-sector organizations, with the goal of grabbing proprietary data and intellectual property.

A related trend is the steady rise of organized cybercrime online. This is entirely logical. As the exchange of money and information has moved online, organized crime has followed, focusing on theft of valuable assets such as intellectual property. This has spawned a mature malware industry that increasingly resembles the legitimate software industry, complete with a broad set of services, guarantees, and price competition among suppliers.

Stealthy Malware

This evolving set of threat agents is using new, more sophisticated tools and methods to mount attacks. Once upon a time, attackers were amateurish—often driven by personal motives such as the prestige of bringing down a big company's network. Accordingly, the arrival of malware on a user's machine was easy to detect: the malware announced itself with icons or messages, and the system often became unusable.

Now the trend is toward malware that is stealthy and uses sophisticated techniques to avoid detection. Attackers plant malware that lies undetected over a long period while it captures information. Another common technique is to quietly spread malware by injecting malicious code into an unsuspecting company's web site; users who visit the site then unknowingly download the code onto their systems.

Accompanying this is a shift from spam mass e-mails to carefully crafted attacks aimed at individuals or specific groups: so-called *spearphishing*. These typically use social engineering techniques, such as providing enough contextual or personal information in an e-mail to tempt people to download malware or click on a link to an infected web site created specifically for that purpose.

Though more expensive to mount, spearphishing attacks are growing because they can be enormously profitable to cybercriminals. In a report entitled "Email Attacks: This Time It's Personal," Cisco Security Intelligence Operations (2011) noted that gains from traditional mass e-mail attacks shrank by 50 percent to USD 500 million due to a number of factors, including the enforced shutdown of several major spam operations. Meanwhile, spearphishing attacks, which can net ten times the profit of a mass attack, tripled, and personalized malicious attacks increased fourfold, costing organizations worldwide about USD 1.29 billion annually—more than double the overall financial impact of mass e-mail attacks. We can expect these stealthy and targeted attacks to continue, with new methods emerging as necessary to circumvent defenses.

Compromise Is Inevitable

The result of this intersection of trends—increasingly sophisticated attackers and methods combined with the enormous proliferation of devices and information—is that traditional prevention methods such as firewalls are no longer adequate. In fact, enterprises need to assume that compromise is inevitable; no defenses can be entirely effective.

I've summarized the reasons why in the following Six Irrefutable Laws of Information Security (with acknowledgements to Culp [2000], Venables [2008], Lindstrom [2008], and other sources):

- Law #1: *Information wants to be free*. People want to talk, post, and share information—and they increase risk by doing so. Some examples:

  A senior executive at a major technology company updated his profile on a business social networking site. In doing so, he inadvertently pre-announced a shift in his employer's strategy—a mistake that was promptly and gleefully picked up by the press.

  An employee found a novel way to fix a piece of equipment more quickly, and—to help others across the company—decided to videotape the procedure. Because video files are so large, it didn't make sense to e-mail the video, so the employee posted it online. Unfortunately, by doing so, he exposed confidential information.

  At one time or another, many people have experienced this disconcerting event: when composing a message, the e-mail software helpfully autofills the address field, but it selects the wrong name from the address book. You hit send without realizing the error, thus dispatching a company-confidential message to someone outside the organization.

  It's worth noting that that this rule is not new. Information has always wanted to be free: think of the World War II slogan "loose lips sink ships." People communicate, and sometimes they share more information than they should. It's just the methods that have changed—and the fact that, with the Internet, a carelessly mentioned detail is instantly available to anyone across the globe.

- Law #2: *Code wants to be wrong*. We will never have 100-percent error-free software. In fact, the more widely used the software, the more malicious individuals will hunt for vulnerabilities in the code. They have found and exploited errors in the world's most widely used web sites, productivity applications, and enterprise business software.

- Law #3: *Services want to be on*. On any computer, some background processes always need to be running, and these can be exploited by attackers. These could even be security software processes used for everyday activities like keeping systems up-to-date with software patches or monitoring for malware.

- Law #4: *Users want to click*. People naturally tend to click when they see links, buttons, or prompts. Malware creators know this, and they take advantage of it. In fact, the entire phishing industry is based on the assumption that users will click on enticing e-mails, web sites, or pop-up ads, triggering the download of malicious code to their systems. The evolution of highly targeted attacks such as spearphishing has taken this to a new level, as when e-mails purporting to be letters discussing legal action from a circuit court were sent to senior executives at a number of companies.

- Law #5: *Fake antivirus software—designed to actually spread viruses and malware—is becoming a growing menace online*. Posting such fake software on the Web is proving to be an effective way for bad guys to get users to install malware on work and home PCs. According to Google researchers, fake antivirus software accounted for 15 percent of malicious content detected on web sites in a recent 13-month period (Rajab 2010).

  Even a security feature can be used for harm. Security tools can be exploited by attackers, just like other software. This means that laws 2, 3, and 4 are true for security capabilities, too.

  According to the *San Francisco Chronicle* (Van Derbeken 2008), the network engineer who built San Francisco's new multimillion-dollar computer network locked the city out of its own network—refusing to divulge the passwords—when he heard about impending layoffs.

  More recently, the systems of a well-known provider of security certificates were compromised. Beyond announcing that the compromise had occurred, the provider didn't share much information about the event, leaving the businesses who had purchased the certificates in an odd position of not knowing whether their systems were secure or not. This is like hearing that your local locksmith has been burgled—without details about exactly was taken—and trying to decide whether you should immediately invest in new locks or wait to see whether you experience an attempted burglary yourself.

- Law #6: *The efficacy of a control deteriorates with time*. Once put in place, security controls tend to remain static—while the environment in which they operate is dynamic. As a result, a control's ability to produce the intended effect diminishes over time, and the effectiveness of the controls progressively degrades.

  This happens for a variety of reasons. Some are internal: there's a tendency to "set and forget"—to install applications and then fail to update them with security patches or to properly maintain access lists.

There are also external reasons for this trend. Recently, researchers at the University of Pennsylvania analyzed the rate at which vulnerabilities were discovered following 700 major software releases (Clark et al. 2010). They found that, in most cases, there was a honeymoon period, averaging about 110 days, during which time relatively few vulnerabilities appeared. After this period, the discovery rate increased exponentially. Their conclusion: the honeymoon essentially represented the hackers' learning curve!

A New Approach to Managing Risk

Given the ever-broadening role of technology and the resulting information-related business risk, we need a new approach to information security built on the concept of protecting to enable. Because compromise is inevitable, managing risk and surviving compromise are key elements of this strategy. This approach should:

- *Incorporate privacy and regulatory compliance by design, to encompass the full scope of business risk*. Also, because technology is now key to every business process, the information security organization must work closely with other business groups to understand and manage risk.
- *Recognize that people and information—not the enterprise network boundary—are the security perimeter*. Information is no longer restricted to tightly managed systems within data centers; it now also resides outside the firewall, on users' personal devices, and on the Internet. Managing risk therefore requires a range of new tools, including user awareness and effective security controls for personal devices.
- Be dynamic and flexible enough to quickly adapt to new technologies and threats. To provide maximum benefit to users, we need to be able to quickly accommodate new devices as they emerge. Our security approach must also be flexible to respond to the changing threat landscape: a static model will inevitably be overtaken by the dynamic nature of threats.

Above all, we need to accomplish a shift in thinking, adjusting our primary focus to enabling the business, and then thinking creatively about how we can do so while managing the risk. Information is the central nervous system of the company. Our role is to provide the protection that enables information to flow freely.